COMBATING FRAUD
Challenges in Managing Fraud Risks in Federally Funded, State-Administered Programs

Statement of Seto J. Bagdoyan, Director,
Forensic Audits and Investigative Service

Testimony

Before the Subcommittee on Government Operations, Committee on Oversight and Government Reform, House of Representatives

For Release on Delivery Expected at 10:00 a.m. ET

Wednesday, April 15, 2026

GAO-26-109093

United States Government Accountability Office

Accessible Version

GAO Highlights

COMBATING FRAUD

Challenges in Managing Fraud Risks in Federally Funded, State-Administered Programs

GAO-26-109093
April 2026
A testimony before the Subcommittee on Government Operations, Committee on Oversight and Government Reform, House of Representatives
For more information, contact Seto J. Bagdoyan at BagdoyanS@gao.gov

What GAO Found

All federal programs and operations are at risk of fraud, regardless of whether they provide financial or nonfinancial benefits or delivery takes place at the federal, state, or local level. Understanding the scope of the problem is critical to combating fraud. In 2024, GAO estimated total direct annual financial losses to the government from fraud at between $233 billion and $521 billion, based on fiscal year 2018 through 2022 data. The estimate captures losses that occur at the state, local, tribal, or other government level if those losses included a federal investigative, administrative, or related action. State agencies administer federal programs, making payment, eligibility, and other decisions. In fiscal year 2025, the federal government provided an estimated $1.2 trillion to state and local governments in federal grants. The programs vary in size, but some, such as Medicaid, involve millions of beneficiaries. Decentralized program delivery such as through distributed payment and eligibility decisions can heighten the risk of fraud.

GAO has previously reported that federal and state program managers' efforts to manage fraud risks have been challenged by weak control environments, data and system limitations, and limited capacity to manage risks. For example, one state agency administering a federally funded program reported it is restricted by state and federal laws from sharing information with other programs in the state, such as information on individuals and their use of state services. This hindered the agency's ability to prevent and detect fraud within and across programs.

Federal programs, including those administered at the state level, are inherently subject to fraud risks from various entities and individuals (see fig.).

Types of Organized Fraud Groups Targeting Government Programs

Sources: GAO analysis of Department of Justice case information and responses from state, federal, and foreign officials (data); Icons-studio/stock.adobe.com and Oleh/stock.adobe.com (icons). | GAO-26-109093

Decentralized program delivery—where federal funds are distributed to grantees, subrecipients, contractors, and subcontractors—creates vulnerabilities to different types of fraud. For example, inspectors general previously reported that the Temporary Assistance for Needy Families block grant to states faced an increased risk of fraud because of limited visibility and control over expenditures at the award recipient and subrecipient levels. Other GAO reporting has shown

that, given the opportunity, organized criminal organizations, businesses, and individuals from all walks of life have sought to defraud federal programs. Certain risk factors—such as program design, culture, and personal motivation—can also increase the risk that fraudsters will target a program.

Why GAO Did This Study

The U.S. federal government is one of the world's largest and most complex entities, spending trillions of dollars across a broad array of programs and operations, with a substantial percentage of this spending administered by the states. The size, scope, and complexity of the federal government create inherent risks that need to be recognized and managed properly.

Fraud is one such risk that must be managed to ensure that program delivery and taxpayer dollars are safeguarded. Every dollar or resource diverted to fraudsters hinders the federal government's ability to achieve its goals. Financial losses also place an increased burden on the government's financial outlook. Fraud also erodes public trust in government and hinders agencies' efforts to execute their missions.

This statement focuses on fraud in federally funded, state-administered programs by (1) outlining the scope of the problem and fraud risk landscape, (2) examining challenges facing federal and state agencies in combating fraud, and (3) examining fraud threats the government faces and why it is difficult to combat them. This statement is based on a body of work of selected reports that GAO issued between 2010 and 2026.

What GAO Recommends

GAO is not making recommendations at this time. As of April 2026, GAO has made 215 recommendations to federal agencies and programs to better manage fraud risks, of which about 40 percent remain open.

Chairman Sessions, Ranking Member Mfume, and Members of the Subcommittee:

I appreciate the opportunity to discuss fraud against federally funded, state-administered programs and the reasons for continued challenges in combating such fraud.

The federal government is one of the world's largest and most complex entities, spending trillions of dollars across a broad array of programs and operations. The size, scope, and complexity of the federal government create inherent risks that need to be recognized and managed properly. Fraud is one such risk that must be better managed to ensure that program delivery and taxpayer dollars are safeguarded.

State agencies administer several federal benefits programs, making payment, eligibility, and other decisions. For example, states administer Medicaid and Unemployment Insurance (UI). In addition, the federal government provides funding to state and local governments through grants, funding a wide range of public policy initiatives. In fiscal year 2025, federal grant funds totaled an estimated $1.2 trillion to state and local governments.[1] Decentralized program delivery of federal programs, such as through distributed payment and eligibility decisions, can heighten the risk of fraud.

Most federal spending, including that administered through states, is not lost to fraud. However, every dollar or resource that is diverted to fraudsters hinders the federal government's ability to achieve its goals. Direct financial losses from fraud place an increased burden on the government's financial outlook.[2] Additionally, nonfinancial impacts and losses erode public trust in government and hinder agencies' efforts to execute their missions and program objectives effectively and efficiently.

While it is impossible to eliminate fraud completely, managing the risk strategically by implementing preventive, detective, and response controls is imperative. And prevention is key—attempting to investigate and prosecute our nation's way out of the problem addresses only a small fraction of fraudulent activity, requires significant time and resources, and returns pennies on the dollar. Further, fraudsters' tactics are ever evolving and so should the U.S. government's approach. To be clear, the task of managing fraud risks is never-ending. The goal is to continuously improve antifraud efforts—through analytics, evaluation, and culture—to more efficiently and effectively prevent fraud upfront, before the loss or compromise occurs.

This statement focuses on fraud in federally funded, state-administered programs by (1) outlining the scope of the problem, the federal fraud risk landscape, and fraud risks in federal programs administered by states; (2)

[1]Congressional Research Service, *Federal Grants to State and Local Governments: Trends and Issues*, R40638, (Washington, D.C.: June 26, 2025).

[2]We have previously reported that the federal government faces an unsustainable, long-term fiscal future. GAO, *The Nation's Fiscal Health: Strategy Needed as Debt Levels Accelerate,* GAO-25-107714 (Washington, D.C.: Feb. 5, 2025). We have also reported improved efforts to combat fraud, with an emphasis on prevention, can reduce the loss of federal dollars and help improve the federal government's fiscal outlook.

examining challenges facing federal and state agencies in combating fraud; and (3) examining fraud threats the government faces and why it is difficult to combat them.

This statement is based on a body of work of selected reports we published from July 2010 to March 2026 addressing fraud risk management.[3] More detailed information on the scope and methodology of our prior work can be found within the individual reports on which this statement is based. These reports are listed in the Related GAO Products page at the end of this statement. We conducted the work on which this statement is based in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We conducted our related investigative work on which parts of this statement are based in accordance with standards prescribed by the Council of the Inspectors General on Integrity and Efficiency.

Scope of Fraud in Federal Programs and Risks to Programs Administered by States

No area of the federal government is immune to fraud. All federal programs and operations are inherently at risk, regardless of whether they provide financial or nonfinancial benefits or whether delivery takes place at the federal, state, or local level.[4] Decentralized program delivery and distributed control environment for programs that are federally funded and state administered pose further challenges to managing fraud risks.

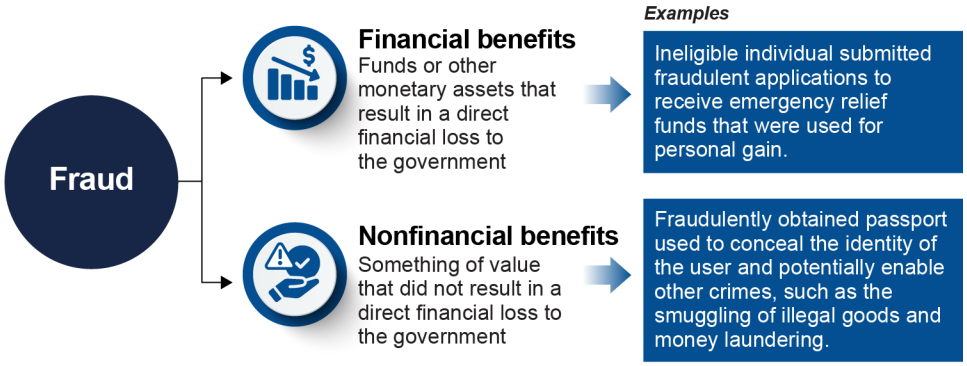
Federal Fraud Risk Landscape

The federal government is a major target for fraud. Fraud schemes are wide-ranging and occur when something of value is obtained through willful misrepresentation. For example, receiving a benefit or assistance from the federal government by lying to meet eligibility requirements is a fraudulent act. Fraud can include financial and nonfinancial benefits, which can have both financial and nonfinancial impacts (see fig. 1).

[3]As of April 2026, we have made 215 recommendations to federal agencies and programs to better manage fraud risks, of which about 40 percent remain open.

[4]Two large federal programs administered by states—Medicaid and Unemployment Insurance—are included on GAO's High Risk List. The High Risk List highlights federal programs and operations that we have determined are in need of transformation. It also names federal programs and operations that are vulnerable to waste, fraud, abuse, and mismanagement. We update our High-Risk List every 2 years at the start of each new Congress. GAO, *High-Risk Series: Heightened Attention Could Save Billions More and Improve Government Efficiency and Effectiveness,* GAO-25-107743 (Washington, D.C.: Feb. 25, 2025).

Figure 1: Examples of Financial and Nonfinancial Benefit Fraud



Sources: GAO (information); Icons-Studio/stock.adobe.com (icons). | GAO-26-109093

Understanding the scope of the problem and the impacts of both financial and nonfinancial benefits fraud are critical to combating it in government programs and operations.

In this regard, fraud risk increased significantly during the COVID-19 pandemic, when the federal government provided about $4.5 trillion in relief funds for response and recovery efforts. The emergency environment and the need to distribute the funds quickly provided increased opportunities for fraud against federal programs, including those that are state administered.

Financial fraud loss. In 2024, we estimated that the federal government loses between $233 billion and $521 billion annually to fraud, based on data for fiscal years 2018 through 2022.[5] The range represents 3 percent to 7 percent of average federal obligations during that period.[6] The width of the range is a reflection of both the uncertainty associated with estimating fraud and the diversity in the risk environments that were present in fiscal years 2018 through 2022. Given the time frame of the data, the estimate includes pandemic-related spending. The estimate also captures losses that occur at the state, local, tribal, or other government level if those losses included a federal investigative, administrative, or related action.[7]

Other estimates of pandemic fraud loss that we and the oversight community developed further support the finding of higher fraud risk in pandemic spending.[8] One such fraud estimate we developed is for UI programs

[5]GAO, *Fraud Risk Management: 2018-2022 Data Show Federal Government Loses an Estimated $233 Billion to $521 Billion Annually to Fraud, Based on Various Risk Environments,* GAO-24-105833 (Washington, D.C.: Apr. 16, 2024).

[6]These percentages should not be applied at the agency or program level.

[7]The upper range of the estimate is associated with higher-risk environments like we saw in the pandemic, whereas the lower end reflects lower risk environments. GAO-24-105833.

[8]We estimated pandemic unemployment insurance fraud to be between $100 billion and $135 billion. GAO, *Unemployment Insurance: Estimated Amount of Fraud during Pandemic Likely Between $100 Billion and $135 Billion*, GAO-23-106696 (Washington, D.C.: Sept. 12, 2023). The Small Business Administration Office of Inspector General (OIG) estimated fraud in two pandemic programs to be about $200 billion. Small Business Administration, *COVID-19 Pandemic EIDL and PPP Loan Fraud Landscape*, White Paper Report 23-09 (June 27, 2023). The Pandemic Response Accountability Committee (PRAC) estimated that three pandemic-relief programs disbursed approximately $79 billion in potentially fraudulent payments due to the use by applicants of over 1.4 million potentially stolen or invalid Social Security numbers. These programs were the Small Business Administration's COVID-19 Economic Injury Disaster Loan program and the Paycheck Protection Program, and the Department of Labor's pandemic-related unemployment insurance programs. PRAC, *Fraud Prevention Alert: Pre-Award Vetting Using Data Analytics Could Have Prevented Over $79B in Potentially Fraudulent Pandemic Relief Payments* (Washington, D.C.: June 2025).

that provided federal economic relief through state workforce agencies. Based on statistical sampling and imputation techniques, we estimated that the amount of fraud in UI programs during the COVID-19 pandemic was likely between $100 billion and $135 billion. This is about 11 percent to 15 percent of the total amount of UI benefits paid during the pandemic.[9]

Nonfinancial impacts. Nonfinancial impacts may not pose a direct financial cost but can lead to other potentially harmful outcomes. We have reported that the federal government faces many such risks, including falsified passport and trademark applications, aircraft registrations, and supporting documentation for immigration-related benefit programs cases.[10]

Fraud Risks in Federal Programs Administered by States

There are many reasons and benefits to having federal programs administered through states.[11] However, this approach exponentially increases the scale of government transactions across the states and U.S. territories. The programs can vary in size, but some, such as Medicaid, involve tens of millions of beneficiaries. When payment or eligibility decisions are made outside of federal agencies, fraud risk heightens.[12]

For example, the Council of the Inspectors General on Integrity and Efficiency reported in January 2021 that grant programs—such as the Temporary Assistance for Needy Families (TANF) block grant that is funded by the U.S. Department of Health and Human Services and administered by states—faced an increased risk of fraud, waste, and mismanagement because of limited visibility and control over expenditures at the award recipient and subrecipient levels.[13] Additionally in May 2020 and October 2021, the Mississippi State Auditor announced that multiple individuals affiliated with that state's TANF program potentially misspent, converted to personal use, or wasted more than $77 million of TANF grant funds.[14]

Decentralized program delivery—where federal funds are distributed to grantees, subrecipients, contractors, and subcontractors—also creates vulnerabilities to different types of fraud. For example, in May 2021, we found the decentralized environment makes the Community Development Block Grant Disaster Recovery (CDBG-DR) vulnerable to certain types of fraudulent schemes as money flows from the Department of Housing

[9]GAO's estimate is for the period from April 2020 (first full month of payments from all UI programs) to May 2023 (end of the public health emergency). This estimate covers all 53 states that participated in the regular and temporary UI programs. The 53 number includes the 50 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands. See GAO-23-106696.

[10]See, for example, GAO, *State Department: Undercover Tests Show Passport Issuance Process Remains Vulnerable to Fraud*, GAO-10-922T (Washington, D.C.: July 29, 2010), *State Department: Pervasive Passport Fraud Not Identified, but Cases of Potentially Fraudulent and High-Risk Issuances Are under Review*, GAO-14-222 (Washington, D.C.: May 1, 2014), and *Intellectual Property: Stronger Fraud Risk Management Could Improve the Integrity of the Trademark System,* GAO-24-106533 (Washington, D.C.: Mar. 14, 2024).

[11]Congressional Research Service, *Federal Grants-in-Aid Administration: A Primer*, R42769 (Washington, D.C.: Mar. 5, 2026).

[12]GAO, *COVID-19: Insights and Actions for Fraud Prevention,* GAO-24-107157 (Washington, D.C.: Nov. 14, 2023).

[13]Council of the Inspectors General on Integrity and Efficiency, *The IG Community's Joint Efforts to Protect Federal Grants from Fraud, Waste, and Abuse* (Jan. 2021). State TANF agencies are grant award recipients. TANF subrecipients can include local agencies, nonprofit organizations, and other contracted organizations.

[14]Mississippi Office of the State Auditor, Press Releases (May 4, 2020; Oct. 12, 2021). See also, GAO, *Temporary Assistance for Needy Families: Additional Actions Needed to Strengthen Fraud Risk Management*, GAO-25-107290 (Washington, D.C.: Jan. 28, 2025).

and Urban Development to several entities, including states, before reaching their intended beneficiaries.[15] These schemes include contractors providing false certification of qualifications or eligibility, fraudulently billing after taking a deposit and receiving CDBG-DR funds, and conspiring to influence the procurement process to circumvent competitive bidding controls.

Federal and State Agencies Have Faced Challenges Combating Fraud in Federally Funded Programs

Challenges Faced in Demonstrating Commitment to Combating Fraud

Widespread recognition of the value of fraud risk management and commensurate commitment have been lacking at federal agencies, including those responsible for state administered programs. As we note in GAO's *A Framework for Managing Fraud Risks in Federal Programs* (Fraud Risk Framework), commitment to fraud risk management is a fundamental first step.[16] Commitment—by program managers at federal and at state levels when administering federal programs—means creating an organizational culture and structure conducive to fraud risk management.

Five Principles of Fraud

- There is always going to be fraud. It is a fact that some individuals will look to gain where there is opportunity. Organizations need robust processes in place to prevent, detect, and respond to fraud and corruption.
- Finding fraud is a good thing. If you do not find fraud, you cannot fight it. This requires a change in perspective so the identification of fraud is viewed as a positive and proactive achievement.
- There is no one solution. Addressing fraud needs a holistic response incorporating detection, prevention, and response, underpinned by a strong understanding of risk. It also requires cooperation and collaboration between organizations.
- Fraud is ever changing. Fraud and counter fraud practices evolve very quickly, and organizations must be agile and change their approach to deal with these evolutions.
- Prevention is the most effective way to address fraud. Preventing fraud reduces financial loss and reputational damage. It also requires fewer resources than an approach focused on detection and recovery.

Source: International Public Sector Fraud Forum, Guide to Managing Fraud for Public Bodies, February 2019. | GAO-26-109093

Commitment to fraud risk management must start with leadership, setting the tone at the top that acknowledges fraud risks, commits attention and resources to manage them decisively, and communicates the value of fraud risk management (see sidebar). The objective of fraud risk management is to ensure program integrity by continuously and strategically mitigating the likelihood and impact of fraud. This objective is meant to facilitate achievement of the program's broader mission and strategic goals by helping to ensure that funds are spent effectively, services fulfill their intended purpose, and assets are safeguarded.[17]

[15]GAO, *Disaster Recovery: HUD Should Take Additional Action to Assess Community Development Block Grant Fraud Risks*, GAO-21-177 (Washington, D.C.: May 5, 2021).

[16]GAO, *A Framework for Managing Fraud Risks in Federal Programs.* GAO-15-593SP (Washington, D.C.: July 28, 2015). The framework provides a comprehensive set of leading practices for combating fraud in a strategic, risk-based way, with a focus on prevention.

[17]GAO-15-593SP.

Potential reputational fears that may result in sweeping incidents of fraud "under the rug," are, in fact, the reasons for managing fraud risks proactively. The impacts of unmanaged fraud risks on programs' reputations and the negative publicity can be severe.

Recommendations to designate an entity to lead fraud risk management were among the five key areas of needed actions, according to our analysis of recommendations we made to federal agencies on fraud risk management from July 2015 through December 2022.[18] Our prior work has shown that when agencies formally designate an entity to design and oversee fraud risk management activities, their efforts can be more visible across the agency, particularly to executive leadership. Commitment to fraud risk management is fundamental to sustaining progress in other areas, such as conducting fraud risk assessments, designing effective controls, and continuously monitoring and evaluating antifraud efforts.

Challenges Faced in Various Practices for Managing Fraud Risks

The Fraud Risk Framework also discusses other leading practices for managing fraud risks. More specifically, as part of delivering on program mission, officials should develop robust fraud risk management programs at federal and state levels to manage fraud risks proactively, strategically, and continuously. This involves effective approaches in designing fraud risk management activities, such as controls and data analytics, as well as staff capacity to carry out antifraud efforts based on current knowledge and skillsets.

However, programs have too long relied on the costly and ineffective "pay-and-chase" model, which refers to the practice of attempting to recover funds after payments have been made. This approach was particularly evident during the COVID-19 pandemic for programs administered at the federal level, such as the U.S. Small Business Administration (SBA)'s programs to support small businesses and retain employees, and for programs at the state level to support individuals, such as the Department of Labor's (DOL) UI programs.

Further, weak control environment, data and system limitations, and limited capacity to manage fraud risks have challenged the practices of federal and state program managers to manage fraud risks and build robust programs.

Weak control environment. We have found that federal and state agencies relied on self-attestation or self-certification for individuals and entities to verify their eligibility or identity to receive assistance from some COVID-19 relief programs, in an effort to disburse funds quickly to those in need.[19] Even when program design decisions allow for self-certification, agencies are responsible for designing and implementing control activities to prevent fraud.

Self-certification alone is not sufficient as a fraud control to mitigate misrepresentation. Our prior work examining SBA's Paycheck Protection Program and COVID-19 Economic Injury Disaster Loan program fraud schemes identified (1) ineligible, nonoperating businesses that applied for, and obtained, program funds; (2) legitimate business owners misrepresenting eligibility regarding their criminal record, federal debt, or principal

[18]The five key areas in which federal agencies need to take additional actions are (1) designating an entity to lead fraud risk management, (2) assessing fraud risks, (3) designing and implementing an antifraud strategy, (4) using data analytics to manage fraud risks, and (5) managing fraud risks in emergencies. GAO, *Fraud Risk Management: Key Areas for Federal Agency and Congressional Action,* GAO-23-106567 (Washington, D.C.: Apr. 13, 2023).

[19]GAO-24-107157.

place of residence, among others; and (3) falsification of tax or other documents to obtain more funds.[20] In these instances, recipients falsely self-certified eligibility. As we reported, other fraud controls to mitigate these misrepresentations were either not in place or were not effective for those programs.

Confirming eligibility of individuals receiving benefits, such as by confirming wage information or by verifying identity through data and other checks, are key controls to prevent fraud schemes that rely on mechanisms such as misrepresentation. However, design of such controls and choices in applying them across programs can impact their effectiveness. For example, we have reported that the U.S. Department of Agriculture's (USDA) Food and Nutrition Service (FNS)—in overseeing the implementation of the Supplemental Nutrition Assistance Program at the federal level—recommended a key control to prevent electronic benefit transfer (EBT) fraud schemes. EBT card security tools required an individual recipient to opt-in to use them, but the adoption rates were extremely low. [21] FNS officials and representatives from several stakeholder organizations said that few EBT recipients used these options because they were optional, perceived as difficult to enroll in, or inaccessible. EBT processors reported that only 5 to 10 percent of EBT recipients used these apps through which these tools were available.

Data and system limitations. In 2023, we reported that our prior review of fraud risks and responses across COVID-19 pandemic programs identified challenges related to eligibility and identity, such as lack of information or data systems to confirm eligibility.[22] Further, as part of our 2025 work on organized fraud groups, we found that state officials specifically cited challenges related to data limitations and program delivery.[23] For example, a state official told us that each program is restricted to sharing data within the program. There are also limits to interagency information sharing. For example, one state agency administering a federally funded program reported that it is restricted by state and federal laws from sharing information with other programs in the state, such as information on individuals and the state services they use. This restriction can limit the ability to connect fraudsters to potential fraud within and across state programs. Federal officials also told us that obtaining critical data, such as tax records to verify an applicant's identity or program eligibility, is time and resource intensive while also safeguarding the data.

In June 2022, we reported that state workforce agencies faced significant challenges in modernizing legacy IT systems for delivering UI programs.[24] States consequently faced challenges in scaling aspects of their UI systems, such as applicant identity verification, to meet demand and detect improper payments. Moreover, we reported that flexibility in how states implemented DOL's Pandemic Unemployment Assistance (PUA) program allowed for variation across states in the systems states used for their PUA programs.[25] For example, some states implemented the PUA program within their regular UI systems. This allowed those states to utilize some

[20]GAO, *COVID Relief: Fraud Schemes and Indicators in SBA Pandemic Programs,* GAO-23-105331 (Washington, D.C.: May 18, 2023).

[21]GAO, *Nutrition Assistance: USDA Should Comprehensively Assess Benefit Theft Prevention Measures States Are Implementing,* GAO-25-107964 (Washington, D.C.: Sept. 25, 2025).

[22]GAO-24-107157.

[23]GAO, *Fraud Risk in Federal Programs: Continuing Threat from Organized Groups Since COVID-19,* GAO-25-107508 (Washington, D.C.: Jul. 10, 2025).

[24]GAO, *Unemployment Insurance: Transformation Needed to Address Program Design, Infrastructure, and Integrity Risks*, GAO-22-105162 (Washington, D.C.: June 7, 2022).

[25]GAO, *Pandemic Unemployment Assistance: States' Controls to Address Fraud,* GAO-24-107471 (Washington, D.C.: July 23, 2024).

of the existing controls from those systems. While using legacy systems could allow states to leverage existing controls, if the legacy system had challenges, these could have been worsened by the increased volume of new claims during the pandemic.

In a December 2021 report, the Pandemic Response Accountability Committee (PRAC) cited a state auditor finding that the state's UI system had unresolved deficiencies that created processing issues.[26] For example, increased claims during the pandemic resulted in many applicants encountering technical errors in that state. Similarly, in the same report, the PRAC cited another state auditor finding that the state's UI system was outdated and unable to detect and prevent fraudulent claims automatically.

Other states worked with contractors to set up new systems dedicated to the PUA program with new functionality not available in the systems used for their regular UI programs. Some states faced challenges when implementing new programs, however. For example, according to the December 2021 PRAC report, one state's UI system was based on a mainframe computer from the 1970s. When integrating the newly developed PUA program to operate with the outdated UI system, the state faced increasing system errors that sometimes denied eligible applicants' claims or delays in processing the claims.[27]

Capacity to manage fraud risks. We have previously reported that those making eligibility determinations or payment certifications may have limited experience or training. These limitations heightened the risk of fraud, waste, abuse, and other payment integrity issues across COVID-19 relief programs. For example, in June 2022, we reported that DOL officials cited new and inexperienced staff as one of the factors that provided opportunities for exploitation of UI programs and system vulnerabilities.[28]

Capacity to manage fraud risks also involves the ability to balance program delivery with fraud controls. Multiple state program officials we interviewed during our 2025 work on organized fraud discussed this challenge.[29] For example, state UI program managers discussed the challenge of needing to meet federal program requirements for timely benefit payments with unemployment insurance programs while also implementing fraud controls, such as identity verification. Additionally, according to a state program official, fraud impacted staff's ability to help legitimate program applicants, increasing wait times in that state.

Lastly, competing priorities, workload challenges, and resource constraints have been identified as reasons for federal agencies not conducting regular fraud risk assessments or assessing states' implementation of available tools to manage fraud risks.[30]

[26]Pandemic Response Accountability Committee, *Key Insights: State Pandemic Unemployment Insurance Programs* (Washington, D.C.: Dec. 16, 2021).

[27]GAO-24-107471.

[28]GAO-22-105162; and GAO-24-107157.

[29]GAO-25-107508.

[30]GAO-25-107290; and GAO-25-107964.

Fraud Threats the Government Faces and Why It Is Difficult to Combat Them

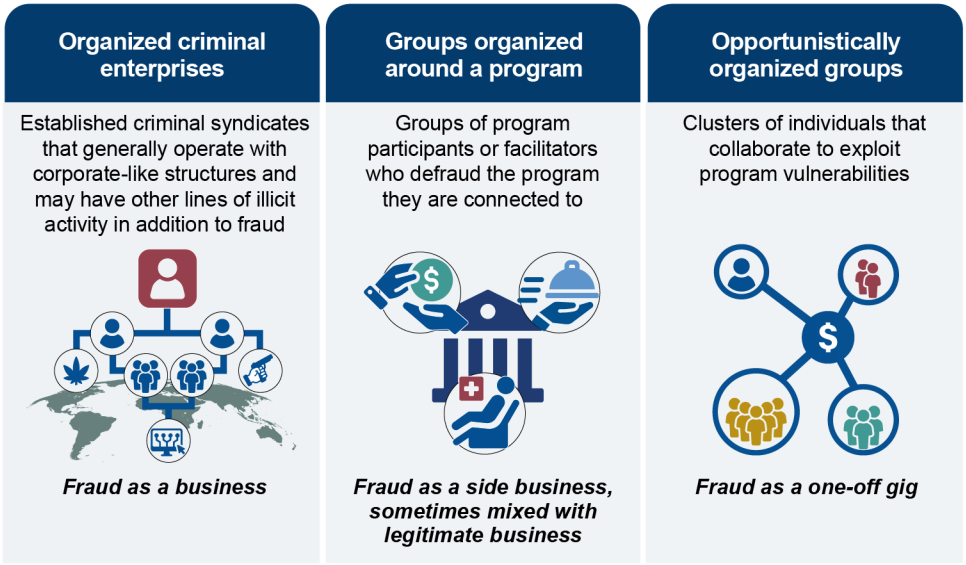
The federal government—including federally funded, state-administered programs—faces a wide variety of fraud threats. Our prior work has shown that, given the opportunity, organized criminal organizations, entities, and individuals from all walks of life have sought to defraud federal programs. Certain risk factors—such as program design, culture, and personal motivation—can also increase the risk that a program will be targeted by fraudsters.

Organized Groups

Organized groups of individuals working together—both domestic and transnational—have defrauded public assistance programs, as was evident during the COVID-19 pandemic.[31] Aided by technology, organized groups have targeted programs at a larger volume and at a greater speed than individuals. As we have reported, organized fraud harms people, programs, and society in many financial and nonfinancial ways that are worsened when carried out on a large scale.

Organized fraud groups that target government programs generally fall into three types and vary in size, structure, and participants. As discussed in our July 2025 report, the types are (1) organized criminal enterprises, (2) groups organized around a program, and (3) opportunistically organized groups (see fig. 2).[32]

Figure 2: Types of Organized Fraud Groups Targeting Government Programs



Sources: GAO analysis of Department of Justice case information and responses from state, federal, and foreign officials (data); Icons-studio/stock.adobe.com and Oleh/stock.adobe.com (icons). | GAO-26-109093

[31]GAO-25-107508.

[32]GAO-25-107508.

Organized criminal enterprises involve established criminal syndicates that may have other lines of illicit activity. Groups organized around a program may involve program participants and facilitators who conspire to defraud the program they are connected to. Opportunistically organized groups involve clusters of individuals who come together as opportunities for fraud arise.

These groups have used technology, program knowledge, and other means to commit fraud on a large scale against government programs. The stages of an organized fraud scheme include methods such as gathering materials and information, defrauding programs on a large scale across multiple regions, evading detection, and laundering fraudulently obtained funds. As we have previously reported, the following examples illustrate how organized groups have defrauded federally funded, state-administered programs.

Organized criminal enterprises. Two foreign nationals and suspected leaders of an overseas-based transnational organized crime group fraudulently obtained UI benefits. In this fraud scheme, the two foreign nationals submitted multiple fraudulent applications to receive UI benefits. They both fraudulently claimed to be U.S. citizens and provided fake Social Security numbers. They used the illicit funds from unemployment benefits, along with funds they received by pawning stolen goods, and laundered these funds through wiring money to entities in another country. Their crimes included robbing $1.4 million in jewelry from residents of elderly communities. Together with their co-conspirators, the two foreign nationals received a total of approximately $32,250 in UI benefits they were not eligible to receive. In 2023, they both pleaded guilty to conspiracy to launder monetary instruments and were sentenced to 30 and 36 months.

Groups organized around a program. In 2020, three pharmacy operators were sentenced for defrauding the USDA's Special Supplemental Nutrition Program for Women, Infants, and Children (WIC). The investigation disclosed that three individuals who operated the pharmacy purchased WIC vouchers from low-income recipients. The pharmacy employed drivers to travel throughout a metro area and purchase high-value special infant formula WIC vouchers from recipients, which the pharmacy operators then redeemed for cash.

Opportunistically organized groups. In October 2024, the U.S. Department of Justice indicted a group for allegedly stealing over $2.4 million in Supplemental Nutrition Assistance Program (SNAP) benefits. The group used those stolen benefits to purchase large quantities of sports drinks and baby formula from websites associated with grocery stores, later reselling the goods on the black market. The group also allegedly evaded eligibility requirements by coercing beneficiaries into selling their benefits, often at a loss. The group then trafficked the illegally purchased benefits loaded onto SNAP EBT cards to third parties, who used the benefits to fraudulently purchase goods. As of April 2026, seven individuals have been sentenced, five individuals pleaded guilty and are awaiting sentencing, four are awaiting trial, and the case against one individual was dismissed.

Other Fraud Opportunists

In addition to organized fraud groups, entities in a wide variety of sectors, and individuals from all walks of life have defrauded public programs. Based on a review of the Department of Justice's pandemic fraud cases, we identified different types of fraudsters who defrauded at least 19 different pandemic-relief programs, both federally and state-administered (see fig. 3).[33]

[33]GAO, *COVID-19 Relief: Consequences of Fraud and Lessons for Prevention*, GAO-25-107746 (Washington, D.C: Apr. 9, 2025).

Figure 3: Types of Opportunists GAO Identified in Pandemic-Relief Program Fraud Cases

Sources: GAO analysis of Department of Justice case information; Icons-Studio/stock.adobe.com (icons). | GAO-26-109093

In 2019, a former operations director of a state child food program was sentenced in federal court to nearly 3 years in prison for defrauding the government and filing a false tax return. The USDA FNS reimbursed the program a set amount per meal served. On a monthly basis, the fraudster's organization submitted requests for reimbursement to the state, which, in turn, received funding from USDA. The fraudster submitted falsely inflated meal count forms; in some instances, they added meals to legitimate counts, and in others, they submitted forms for days when no meals were served at all.

Evolving Fraud Tactics

Efforts by federal and state officials to protect their programs from fraud are often outpaced and outmatched by fraudsters, whose schemes and use of technology are continuously evolving. During our 2025 work on organized fraud, federal and state officials told us that the increased use of stolen identities from data breaches, synthetic identities, and widespread availability of advanced technological tools, such as AI and bots, will continue to pose major challenges for officials who are continuously "one step" behind organized fraud groups.[34] Officials from one agency stated that organized groups increasingly rely on obtaining large volumes of Personally Identifiable Information (PII) from data breaches, phishing attacks, and the purchase of stolen records from the dark web. An official from another agency said that organized groups may use AI and bots to facilitate fraud schemes, allowing them to file claims in rapid succession seconds or minutes apart. The widespread availability of these tools can allow individual fraudsters to operate at a level similar to organized fraud groups.

Chairman Sessions, Ranking Member Mfume, and Members of the Subcommittee, this completes my prepared statement. I would be pleased to respond to any questions that you may have at this time.

[34]GAO-25-107508.

GAO Contact and Staff Acknowledgments

Seto J. Bagdoyan, BagdoyanS@gao.gov

In addition to the contact named above, Irina Carnevale (Assistant Director), Paulissa Earl (Analyst in Charge), Rebecca Shea, Gabrielle Fagan, Nicholas Weeks, and Christopher Klemmer made key contributions to this testimony. Other staff who contributed to this testimony include Colin Fallon, Kristy Hammon, Barbara Lewis, Maria McMullen, Brenda Mittelbuscher, Sabrina Streagle, and Erin Villas.

Related GAO Products

Fiscal Year 2027 Budget Request, GAO-26-900720, Washington, D.C.: Mar. 18, 2026.

Nutrition Assistance: USDA Should Comprehensively Assess Benefit Theft Prevention Measures States Are Implementing, GAO-25-107964, Washington D.C.: Sept. 25, 2025.

High Risk Series: Heightened Attention Could Save Billions More and Improve Government Efficiency and Effectiveness, GAO-25-107743, Washington, D.C.: Feb. 25, 2025.

Fraud Risk in Federal Programs: Continuing Threat from Organized Groups Since COVID-19. GAO-25-107508, Washington, D.C.: July 10, 2025.

COVID-19 Relief: Consequences of Fraud and Lessons for Prevention, GAO-25-107746, Washington, D.C: Apr. 9, 2025.

Pandemic Unemployment Assistance: States' Controls to Address Fraud, GAO-24-107471 (Washington, D.C.: July 23, 2024).

Temporary Assistance for Needy Families: Additional Actions Needed to Strengthen Fraud Risk Management, GAO-25-107290, Washington D.C.: Jan. 28, 2025.

The Nation's Fiscal Health: Strategy Needed as Debt Levels Accelerate, GAO-25-107714, Washington, D.C.: Feb. 5, 2025.

COVID-19: Insights and Actions for Fraud Prevention. GAO-24-107157, Washington, D.C.: Nov. 14, 2023.

Intellectual Property: Stronger Fraud Risk Management Could Improve the Integrity of the Trademark System. GAO-24-106533, Washington, D.C.: Mar. 14, 2024.

Fraud Risk Management: 2018-2022 Data Show Federal Government Loses an Estimated $233 Billion to $521 Billion Annually to Fraud, Based on Various Risk Environments. GAO-24-105833, Washington, D.C.: Apr. 16, 2024.

Unemployment Insurance: Estimated Amount of Fraud During Pandemic Likely Between $100 Billion and $135 Billion. GAO-23-106696, Washington, D.C.: Sept. 12, 2023.

Fraud Risk Management: Key Areas for Federal Agency and Congressional Action. GAO-23-106567, Washington, D.C.: Apr. 13, 2023.

Unemployment Insurance: Data Indicate Substantial Levels of Fraud during the Pandemic; DOL Should Implement an Antifraud Strategy. GAO-23-105523, Washington, D.C.: Dec. 22, 2022.

COVID Relief: Fraud Schemes and Indicators in SBA Pandemic Programs. GAO-23-105331, Washington, D.C.: May 18, 2023.

Disaster Recovery: HUD Should Development Data Collection Guidance to Support Analysis of Block Grant Fraud Risks, GAO-23-104382, Washington, D.C.: Aug. 17, 2023.

Unemployment Insurance: Transformation Needed to Address Program Design, Infrastructure, and Integrity Risks, GAO-22-105162, Washington. D.C.: Jun. 7, 2022.

Disaster Recovery: HUD Should Take Additional Action to Assess Community Development Block Grant Fraud Risks. GAO-21-177, Washington, D.C.: May 5, 2021.

A Framework for Managing Fraud Risks in Federal Programs. GAO-15-593SP, Washington, D.C.: July 28, 2015.

State Department: Pervasive Passport Fraud Not Identified, but Cases of Potentially Fraudulent and High-Risk Issuances Are under Review, GAO-14-222, Washington, D.C.: May 1, 2014.

State Department: Undercover Tests Show Passport Issuance Process Remains Vulnerable to Fraud. GAO-10-922T, Washington, D.C.: July 29, 2010.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or
TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on X, LinkedIn, Instagram, and YouTube.
Subscribe to our Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454

Media Relations

Sarah Kaczmarek, Managing Director, Media@gao.gov

Congressional Relations

David A. Powner, Acting Managing Director, CongRel@gao.gov

General Inquiries

https://www.gao.gov/about/contact-us